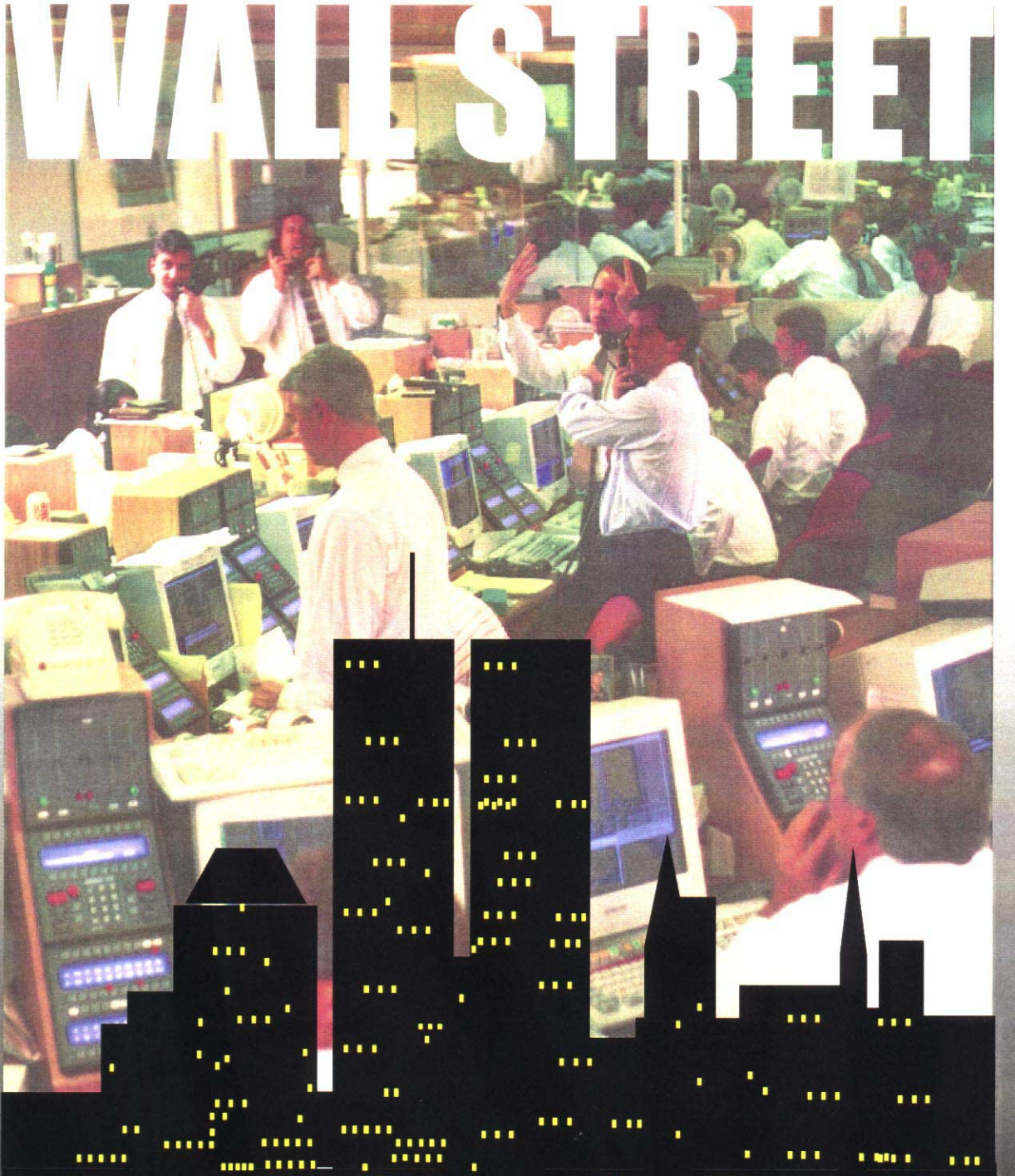
WALL STREET



Economic Security Exercise

Co-sponsored by

United States Naval War College

and

Cantor Fitzgerald

THE VICE PRESIDENT
WASHINGTON

October 25, 1997

Economic Security Exercise
New York, New York

Dear Friends:

I am pleased to send my personal greetings to everyone participating in the Economic Security Conference, sponsored by the Naval War College. While I regret that I am unable to join you, I do want to extend my best wishes for a successful and productive event.

As we journey into the next century, we are finding that national security and economic security are becoming inextricably linked. America has taken great steps to protect our citizens and our borders from physical attack; we must become equally vigilant concerning threats to the security of our National Information Infrastructure (NII). New risks to the NII have emerged as the result of the rapid proliferation and integration of computers connecting infrastructures to one another in a complex network of interdependence. To address this issue, the President created the Commission on Critical Infrastructure Protection, which reported its recommendations to the Administration last Monday.

The President's Commission found no evidence of imminent threats to our infrastructures. However, capabilities exist today to exploit our vulnerabilities and create unacceptable levels of harm to our infrastructure. By acting today, in partnership, we can head off this threat to our safety and economic competitiveness. We cannot afford to wait and let the seriousness of an attack upon our infrastructure be demonstrated for us. The exercise you are participating in will examine critical areas regarding the potential vulnerabilities of this network of networks, and ways in which we can address these vulnerabilities.

Since most of the infrastructures examined in the report are privately held and not government owned, the creation and expansion of a public-private partnership is an essential prerequisite toward addressing broad threats to our economic security. I am particularly pleased to hear that the Naval War College is working with other government departments and key members of the financial community to address these issues. The group gathered for this exercise represents an important cross section of leaders needed to face the challenge this threat poses for America. I know that Admiral Cebrowski, Mr. Richard Clarke of the National Security Council, Congressman Stearns and Congressman Schumer--along with the rest of you--share a deep concern for protecting our information infrastructure.

I want to thank you for this opportunity to address the first economic security conference. I also want to thank Admiral Stark and Mr. Lutnick for their kind invitation and for making this forum possible. Certainly, I look forward to hearing of the results of this important exercise in the near future.

Once again, please accept my warmest regards during this special occasion.

Sincerely,

Al Gore

AG/cco

I. Introduction

A. Welcome

On behalf of Rear Admiral James Stark, USN, President of the United States Naval War College, and Mr. Howard Lutnick, President and CEO of Cantor Fitzgerald, we welcome you to the Economic Security Exercise.

For decades, the Naval War College has led the defense community in gaming and simulation to underpin military plans and requirements. As we look to the future, we intend to include insights of experts in the financial community as a key part of our planning.

B. Purpose and Objectives

The worlds of international politics, national security, and financial markets are tightly linked. This Exercise brings together key figures from the national security, political, governmental and regulatory, and financial communities to explore and test the relationships between international politics, national security, and financial markets. The overall purpose of the Exercise is to reach conclusions between the various communities regarding the implications of potential crises and ways to hedge against their impact. In particular, we will together:

- explore the financial implications of a conflict in Southwest Asia that threatens to close the Straits of Hormuz and subsequent attacks on infrastructure critical to business and finance
- discuss measures the financial community and the US Government can take to prevent or mitigate the consequences of these threats

In this Exercise book, we provide the background information you should be aware of prior to the Exercise itself on Saturday, 25 October.

C. Where, when, and other Exercise particulars

1. Reception, dinner, and opening discussions

We will start the Exercise with a reception and dinner on Friday, 24 October, at Windows on the World, One World Trade Center, 106th Floor. Dress will be business attire. Upon arrival at One World Trade Center, we will give participants badges for access to the 106th floor. Sponsored by Cantor Fitzgerald, the reception will begin at 6 p.m. (or 1800, for those who want to get into the military command and control aspects of the Exercise). After we move into the room for dinner, Rear Admiral James Stark and Mr. Howard Lutnick will give opening remarks. Following dinner, Dr. Tony Lake and Dr. Stuart Starr will brief participants on the scenarios for the Exercise. Mr. David Rothkopf, Representative Clifford Stearns, and Mr. Bob Fauver will comment. We will then have open discussions and adjourn no later than 10 p.m. (2200).

2. The Economic Security Exercise

We will check-in participants on the 106th floor beginning at 9 a.m. (0900) on Saturday, 25 October. Exercise play will begin at 9:30 a.m. (0930), continue through a working lunch, and conclude no later than 5:00 p.m. (1700). Dress will be casual.

During the dinner and Exercise, participants may receive messages at the following numbers:

Windows on the World: Phone 212-524-7000 ; Fax 212-524-7016
Exercise: Phone 212-524-7106; Fax 212-524-7016
Cell phones will not be allowed.

3. Schedule

Friday, 24 October

1800 Reception
1900 Dinner / Welcoming Remarks
2000 Setting the Context: Briefings, Comments, and Discussion
2200 Adjourn

Saturday, 25 October

0900 Check-in / Refreshments
0930 Southwest Asia Scenario
1145 Working Lunch
1230 Summary Discussion, Southwest Asia Scenario
1330 Information Warfare Scenario
1500 Summary Discussion, Information Warfare Scenario
1600 Discussion: What should be done? By Whom?
1700 Adjourn

4. Questions?

Please feel free to address questions to any of the Naval War College staff listed in the "Who's who" section during the Exercise. If after the Exercise you have any remaining questions, please call Dr. Lawrence Modisett, Director, Decision Support Department, Naval War College, at 401-841-4057, his secretary Avon Teague at 401-841-1798, or the Exercise analyst (and principal author of this Exercise book) Professor Jeffrey Sands at 401-841-3139.

II. Who's who

We will be handing out the layout and seat assignments at the Exercise itself. The tables that follow provide a full listing of Exercise participants and gallery, with brief commentary on backgrounds or roles in the Exercise.

Exercise Participants

Conference Hosts	Rear Admiral James **Stark**, USN	President, Naval War College
	Mr. Howard **Lutnick**	President and CEO, Cantor Fitzgerald
Political and National Security Experts	Prof. Paul **Bracken**	Yale University, School of Management
	Vice Admiral Arthur **Cebrowski**, USN	Acting Vice Chief of Naval Operations; Director, Space, Information Warfare, Command and Control (N-6)
	Hon. Richard **Clarke**	Special Advisor to the President and Senior Director for Global Affairs, National Security Council
	Mr. Roger **Cressey**	Office of the Assistant Secretary of Defense for Strategy and Resources
	The Hon. Clifford **Stearns**	Member of Congress
Economic and Monetary Policy Experts	Mr. Robert **Fauver**	National Intelligence Officer, Global Economic Issues
	Mr. James **Hart**	Office of International Energy Policy, Department of Energy
	Ms. Deborah **Perelmuter**	NY Federal Reserve, Open Market Desk
	Mr. Gary **Rasmussen**	Director, Office of Market Finance, US Treasury
	Mr. David **Rothkopf**	Kissinger Associates; former Under-Secretary of Commerce for International Trade
Information Warfare Experts	Mr. Randy **Beers**	National Security Council
	Dr. Stuart **Starr**	Director of Planning, MITRE Corp.
Financial Community	Mr. Mark **Bavosa**	Dean Witter Intercapital
	Mr. Alfred **Berkeley**, III	The NASDAQ Stockmarket, Inc.
	Mr. John **Cadley**	JP Morgan Securities, Inc.
	Mr. Neil **De Sarno**	CIBC Wood Gundy Securities Corp.
	ADM William "Bud" **Flanagan**, USN (Ret)	Cantor Fitzgerald; former Commander in Chief, US Atlantic Fleet
	Mr. Irving **Goldman**	CS First Boston
	Mr. Thomas **Gribbon**	The Nikko Securities Co. International
	Mr. Kent **Karosen**	Cantor Fitzgerald
	Mr. Richard **Kelly**	Aubrey G. Lanston and Co., Inc.
	Mr. Mark **Mahoney**	UBS Securities, LLC
	Mr. Stephen **Merkel**	Cantor Fitzgerald, General Counsel
	Mr. George **Pratt**	Paribas Corporation
	Mr. Lewis **Sonn**	Financial investor
Naval War College	Prof. Bud **Hay**	Naval War College, War Gaming Chair, Exercise Co-Facilitator
	Dr. Stuart **Johnson**	Naval War College / RAND, Exercise Facilitator

Exercise Gallery

Mr. Frank **Aquilino**	Cantor Fitzgerald
Captain Scott **Cubbler**, USMC	Public Affairs Officer, USMC, New York
Major General Donald **Gardner**, USMC (Ret)	Intrepid Museum Foundation
CDR Kevin **McIntire**, USN	Naval War College, Exercise Logistics Coordinator
Dr. Lawrence **Modisett**	Naval War College, Exercise Coordinator
Prof. Jeffrey **Sands**	Naval War College, Exercise Analyst
CDR Paul **Schmidle**, USN	Naval War College, Exercise Technology Director
CDR Gary **Shrout**, USN	Naval War College, Public Affairs Officer
Mr. William **White**	Intrepid Museum Foundation
Ms. Helen **Williams**	Cantor Fitzgerald

III. Scenarios

The Exercise will be in two parts, both scenario-based. The first part will focus on a regional crisis in the Persian Gulf region, with the second part a series of nearly simultaneous Information Warfare attacks against key infrastructure nodes in the United States. Both scenarios take place in February-March 2000 in the midst of the United States Presidential primary season. Here, we provide the background for each scenario and the first move for the regional scenario; we will inject additional moves during the Exercise itself.

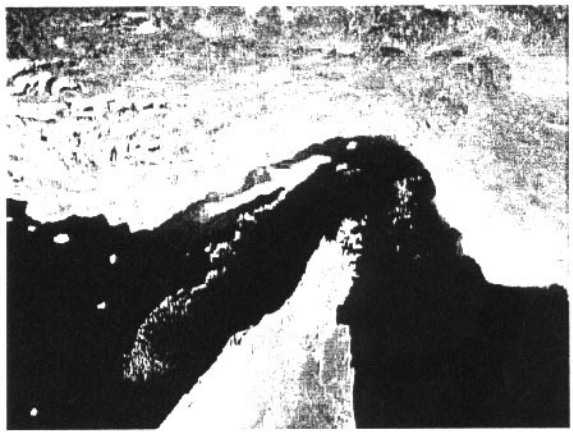
A. Regional Scenario

At each stage in the regional scenario, we will ask participants to gauge the impact of events on US and world markets. For example, participants will identify the impact of the scenario on:

- Exchange rates; e.g.,
  - the value of the Yen relative to the US dollar (122 baseline)
  - the value of the Mark relative to the US dollar (1.9 baseline)
- Equity markets
  - the Dow Jones Industrial Average (10,000 baseline)
- Treasury rates, e.g.,
  - the 30-year Treasury Bond yield rate (6.25% baseline)
  - the three month T-Bill interest rate (5% baseline)
- Commodity prices, e.g.,
  - the Spot West Texas Intermediate ($21 baseline)
  - Gold ($350/oz baseline)

We will develop a consensus among participants at the beginning of the Exercise of the right indices to examine during the moves. In a wrap-up discussion of this scenario, we will ask participants to identify measures the financial community would want the US government to take to minimize the financial and market impact previously identified.

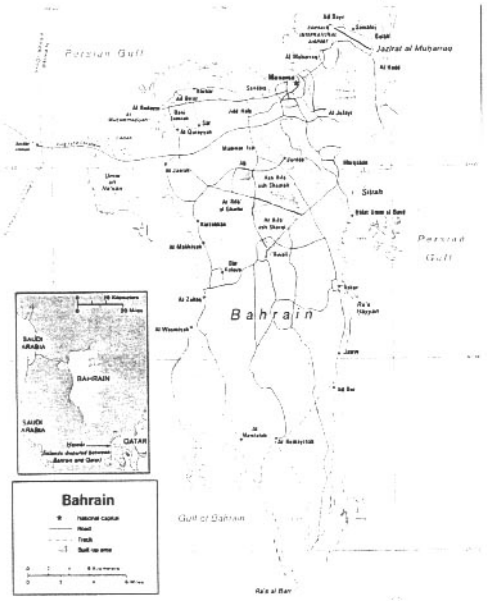
1. Prelude to crisis



Faced with the expanding cultural impact of the West, Muslim leaders throughout the Arabian Peninsula have voiced increasingly strident denunciations of Western culture and influence. Citing Western influence as the cause of economic and social ills, these leaders have led a revival of religious fervor across the Peninsula. Income throughout the Peninsula has not kept pace with growing populations, and all Gulf Cooperation Council countries—including Saudi Arabia—have been unable to satisfy demands for social services and jobs. Hezoballah movements, backed by Iranian funding, training, and rhetoric, are active in Saudi Arabia, Bahrain, Kuwait, Qatar, Oman, and the UAE. These movements are seen by the local populations as pro-nationalist, culturally important elements of Islamist society. All the ruling peninsular monarchies are dealing with Islamist criticism. In Saudi Arabia, the leadership is divided over how to deal with the rising problems. The dominant Saudi policy consideration is how not to fan additional internal dissent or aggravate Iran. As a result, US military access to Saudi bases is threatened.

2. Islamist coup in Bahrain and initial reactions

In a bloody coup d'etat, Islamist radicals seize power in Bahrain. The Emir flees to Riyadh. Tehran immediately recognizes the new regime and announces full support. The United States and Saudi Arabia voice support for the Emir. Significantly, European governments and Japan take no position. No Gulf Cooperation Council states recognize the new regime, and most condemn the coup as an illegal seizure of power.



US intelligence reports the presence of several thousand Iranian troops in Bahrain. Ostensibly there to train the new Islamist Bahraini military, these troops are suspected by the intelligence community to be the vanguard of a larger Iranian-led security force for the new regime. Supported by the Iranian troops, the new Bahraini Islamist military executes a bloody purge of the Emir's supporters. The coup leaders order the US Navy to close all facilities in Bahrain and to leave immediately. While stating that it does not want a confrontation with the United States, Tehran nonetheless declares that it will take whatever means are necessary to support the new regime. The US State Department spokesman denounces the new regime and Iran's role, and threatens a move for sanctions in the United Nations Security Council against both Iran and Bahrain. The Chairman of the Joint Chiefs of Staff briefs reporters on the movement of military assets to the Persian Gulf region.

In Saudi Arabia, demonstrations in Shia areas supporting the Islamist nature of the Bahraini coup are quickly and ruthlessly put down by the Saudi security forces. Responding to the pleas of the Emir and

seeing the new Bahraini regime as a threat to its own domestic stability, Saudi Arabia starts to posture forces to return the Emir to power in Bahrain. Riyadh asks the United States to position forces to restrict Iranian access to Bahrain, stating that it will not be possible to reverse the effects of the coup unless Iran is precluded from reinforcing the new regime.

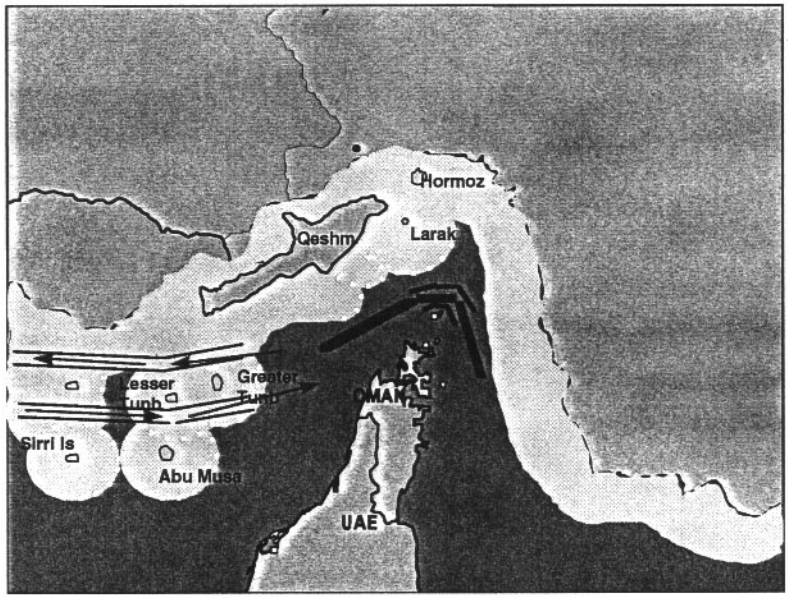
Iran declares that it will not permit the restoration of the Emir to power. Tehran further declares that any deployment of US forces into the region to threaten the new government will be countered by military force and result in the closure of the Strait of Hormuz. Iran commences posturing naval forces and coastal defense missile systems along its coast near the Strait and reinforces its islands in the southern Persian Gulf.

The United States continues to deploy forces into the theater, and the US Fifth Fleet (with its headquarters still in Bahrain) expands patrols in the Strait and the southern Gulf. The White House spokesman calls the situation "extremely serious" and does not rule out the use of unilateral force if necessary.

The other members of the Security Council call for calm while delaying action on the US-proposed sanctions and armed action, if necessary, against Iran and the new regime.

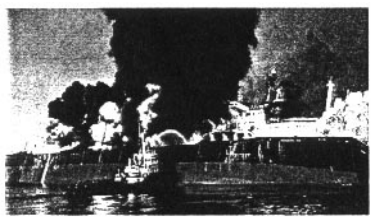
3. Crisis: Focus on the Strait of Hormuz

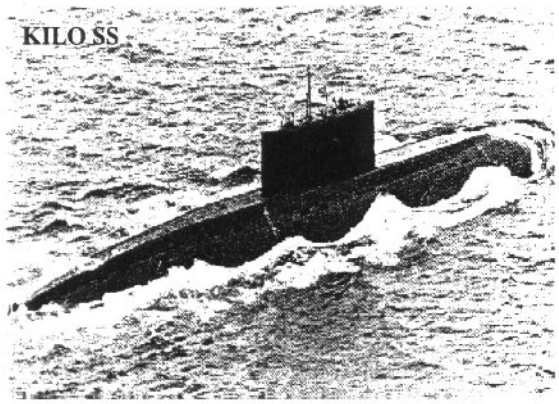
Tehran notifies its populace to prepare for a jihad against the United States and commences a general mobilization of reserve forces. Iran's navy continues increased patrols and its coastal defense and air defense forces are placed on high alert.



A Kuwaiti fishing vessel observes a Dhow dropping mine-like objects in the outbound transit lane.

An outbound Japanese merchant tanker in the transit lane near the Iranian held island of Abu Musa experiences an underwater explosion suspected to be caused by a mine and is heavily damaged. A US Navy patrol detects an Iranian ship mining in the strait and sinks the ship.





Commander, US Naval Forces Central Command reports that Dhows are laying mines in the transit lanes at night. Further, three Iranian Kilo submarines, with mine-laying capability, have sortied from their Bandar Abbas base, joining another Kilo submarine that sortied more than a week ago. All three Kilos are not currently located. Finally, worst-case intelligence estimates are that these submarines could have covertly laid a minefield in the transit lanes. If so, COMUSNAVCENT estimates it would take 30 days to ensure clearance of the lanes.

In response, the US Navy offers to provide escort to US-flagged merchant traffic (with flexible re-flagging arrangements, as in Operation EARNEST WILL in the late 1980s). The Royal Navy echoes this offer.

Iran, of course, denies all responsibility for any of these incidents.

B. Information Warfare

In the second part of the Exercise, participants will consider an extension of the regional scenario in which someone, presumably Iran, has coordinated information warfare attacks against critical infrastructures. Participants will consider various forms of possible attack, assess the impact of each type of attack on commercial operations and markets, and discuss measures the financial community could take in partnership with government to minimize vulnerability to such attacks.

As background to the information warfare portion of the exercise, we enclose a recent speech by Robert Thomas ("Tom") Marsh, Chairman of the President's Commission on Critical Infrastructure Protection. The Commission reported out to the President last week. For those interested, we can make available another of the Chairman's speeches and the Executive Summary of a November 1996 Report from the Defense Science Board (DSB) Task Force on Information Warfare - Defense.

The text of the September 24 speech follows.

Remarks Prepared for Delivery by Robert T. Marsh, Chairman, President's Commission on Critical Infrastructure Protection, New York Federal Reserve, New York, New York , September 24, 1997

Thank you, George [George Juncker, Vice President of Bank Supervisors] and good afternoon, ladies and gentlemen. I am very happy to have the opportunity to participate in this important conference. It is reassuring to know that members of our nation's financial community are acutely aware of the challenges to the security of our telecommunications and information systems, and are actively moving to address them.

I know that you have been discussing security—from overall network security to trends in Internet security—at great length today. I'm going to spend the next few minutes talking about the nationwide security perspective, particularly the security and protection of our nation's critical infrastructures, including the banking and finance industry.

Let me first give you a brief introduction to the Commission and our mission, a review of some of our preliminary recommendations, and then several that relate directly to your community.

In our charter we were directed to consult "with elements of the public and private sectors... and the owners and operators of the critical infrastructures." In keeping with this, it is fitting for me to run some of our ideas by you and invite your reactions.

Background

President Clinton established the Commission last July and charged us to recommend a national policy for protecting and assuring the nation's critical national infrastructures. For just over a year now, we have been working to identify and assess vulnerabilities and threats—and then to develop a national strategy and an implementation plan.

Besides banking and finance, we have been studying and analyzing telecommunications, electric power, oil & gas delivery and storage, transportation, water, emergency services, and government services—those life support systems that the President identified as critical because their incapacity or destruction would have a debilitating effect on our defense and/or economic security. Without electric power and telecommunications, for example, our military could not deploy, our banks could not operate, and our citizens could not enjoy their customary high quality of life.

Critical infrastructures have long been lucrative targets for anyone wanting to do harm to another country. For most of our history, the Atlantic and Pacific Oceans were all the infrastructure protection we needed. But during the Cold War, Soviet and US nuclear weapons were targeted against each other's power grids, road and rail networks, energy industries, and telecommunications systems. And in the Persian Gulf War, disabling Iraq's infrastructures was one of the keys to our success—a lesson noted with interest by many countries in the world.

Clearly there is nothing new about infrastructures being targets. So why was the President motivated to create this Commission at this time?

It was the realization that

- our society was becoming vitally dependent on these infrastructures for its very well-being;
- the infrastructures themselves were becoming increasingly dependent upon information technologies for their functioning;
- they were becoming increasingly interconnected through advances in computers and telecommunications, most especially the Internet, and
- they were consequently becoming increasingly vulnerable to disruption by simple methods readily available to relatively unskilled persons intent on doing harm.
- And there was mounting evidence of such danger by the growing number of malicious cyber incidents throughout the nation with each passing day.

Vulnerabilities and Threats

The Commission was tasked to look at both physical and cyber threats to our nation's infrastructures. We have long understood the physical threat, but the fast pace of technology means we are always one step behind understanding the cyber threat. The Commission has focused on getting ahead of the cyber threat, facing tomorrow's challenges today, and avoiding situations that could cause serious problems in the future.

Our research indicates that the vulnerabilities of our infrastructures are increasing. And this vulnerability information is readily accessible. In fact, our data come almost entirely from open sources, much of it available on the Internet.

Our research has also led us to a new understanding of the threat. Neither the actor nor the intent are known, but we do know that the capability to do harm—the skills and technology necessary—are expansive, and growing, and getting cheaper by the day. And there is no shortage of opportunity for those seeking to do harm. While once an attack on our nation's infrastructures had to overcome physical distance and physical borders, now an adversary can gain access to the heart of our infrastructures from anywhere instantaneously, and can use that instant access to do harm.

There is a whole new arsenal of "weapons of mass disruption" in the cyber world—including viruses, "trojan horses," denial of service, and theft of proprietary data. These tools recognize neither borders nor jurisdictions. They can be used anywhere, anytime, by anyone with technology commonly found in an average college dorm room.

A few examples should illustrate the power of bad actors using new tools.

- Langley Air Force Base, just outside Washington DC, and several government and academic sites—all of which prided themselves on their tight information security regimes—were targets of a recent e-mail attack. A flood of e-mail messages originating in Australia and Estonia—and routed through the White House computer system among others—virtually shut down the Air Base's e-mail for hours until network administrators could construct programs which filtered out the "bad" e-mail messages.
- The 911 system in Miami suffered a similar "denial of service" attack when its phone lines were intentionally flooded with calls.

- And we have all heard of regional Internet service providers being "down" for several hours—sometimes by deliberate actions to deny service—a problem made ever more serious with the growing number of businesses and government services relying on the Internet for day-to-day business transactions.

Given this new geography—in which information is power—the Commission has concentrated on understanding what is needed to protect and assure our nation's critical infrastructures in the cyber age.

The Partnership

The Commission was uniquely tailored for this task. In recognition that the critical infrastructures are largely owned and operated by the private sector, the Commission is a joint public and private venture. Half the Commissioners are full-time career government senior executives, and half are senior representatives from the private sector who have agreed to serve one year as full-time government employees.

A Presidentially-appointed Advisory Committee of key industry leaders provides the unique perspective of owners and operators of the infrastructures as they assist and advise us. And a Steering Committee of senior government officials, including the Attorney General, helps us weave our way through the tangled web of governmental equities.

As part of our consultation efforts, we met with more than 5,500 individuals, corporations, associations, and government agencies around the country. We held five public meetings where we spoke with hundreds of people from industry, academia, science, technology, the military, and government.

Our goal all along has been to create a public-private partnership to protect our future. Government alone cannot address the problem. My aim here today is to further promote that partnership.

"Core" Recommendations

I would like to start by sharing with you a few of our core recommendations. These are ones that cut across all the infrastructures, then follow with a few that may be of particular interest to you in the banking sector. I hope you will be pleasantly surprised not to hear recommendations that call for more regulation or tighter laws.

Information Sharing / National Structures

One of our toughest problems—across all infrastructures—is the sharing of information. There is already a heavy volume of information passed by industry—especially banks, as you well know—to government as part of the regulatory process and in support of law enforcement.

But managing the new risks inherent in an information-based society requires a different type of information exchange within the industry and between industry and government. We do not mean more burdensome regulatory demands. We do mean a cooperative, collaborative environment in which business and government participate in a two-way exchange of information focused on protecting our infrastructures.

Managing these new risks calls for partnership at many different levels, from policy-making aimed at preventing a crisis through responding if such a crisis occurs. Our goal is not to supersede existing relationships you might have with law enforcement or other government agencies, but to establish the appropriate channels that best accommodate the cyber threat.

The Commission has some specific proposals to facilitate 1) identifying the information needed to best protect our infrastructure and 2) sharing—while protecting—that information. These recommendations lay the foundation for a "trusted environment" necessary for achieving the public-private partnership essential for protection into the next century.

At the policy-making level, we will recommend a very high level council comprised of senior CEOs from throughout the critical infrastructures, meeting regularly with selected Cabinet Officers. This National Infrastructure Assurance Council would propose policies and focus attention on infrastructure concerns. The purpose is to open the door of policy formulation to include the private sector infrastructure owners and operators—those that are closest to the problem and best know the range of solutions.

At the operating level, our recommendations focus on enhancing industry and government's information exchange, including

- Organizing Sector Infrastructure Assurance "clearinghouses"—most likely an existing association or industry group—that best suit each infrastructure's information-sharing needs. In essence, each industry will select an entity to coordinate that industry's various participants—such as the financial service companies, exchanges, payment systems, investment companies, and banks that comprise the financial industry—and to identify, collect, desensitize, and disseminate necessary information related to infrastructure protection.
- Designated Federal Agencies will be tasked to facilitate establishing these clearinghouses and provide any necessary government support.
- Creating a public-private Information Warning and Analysis Center staffed by both government and industry representatives. Their job will be to receive relevant information from the sector clearinghouses and various government agencies, analyze this information to assess what is happening in the infrastructures, decide on the necessary protective measures to be taken, determine best practices, and disseminate needed information to both government and industry.

Key to success will be protecting privileged information from both government and the private sector from unauthorized disclosure. This public-private organization must embody the trust essential for the partnership between government and the owners/operators for successful infrastructure assurance.

Clearly, we strongly endorse a policy of reliance on the private sector for problem-solving, solutions, and technology. But we also see a need for government to create a strong focal point for infrastructure protection. Thus we are proposing a high-level advisory position to the President, along with a small staff to coordinate the federal government's infrastructure assurance program and support and interact with the National Council.

The sum of these efforts is to create flexible, reliable channels for information to flow between decentralized private industry and centralized government organizations. In essence, the federal lead agencies will be the "adapter plug" from government to industry—to facilitate the flow of government information to the private sector—and the Sector Infrastructure Assurance clearinghouses will be the "adapter plugs" in the opposite direction—to facilitate the flow of private sector information to the government.

Research & Development

We found that research and development efforts by the federal government are inadequate to deal with emerging cyber threats. Only about $250 million per year is being spent on federal infrastructure-related R&D, of which 60 percent—or $150 million—is dedicated to information security. There is very little R&D effort on the types of real-time detection, identification, and response tools that the Commission believes are necessary. We concluded that market demand is currently insufficient to spur that which is required over the longer term. Consequently, we recommend a doubling of federal funding for R& D in this area to $500 million per year.

Education and Awareness

Key to the success of these initiatives is educating all the stakeholders about the emerging threats and vulnerabilities in the cyber dimension. The Commission's recommendations are aimed at all levels of education, from graduate programs to grammar school. The Commission will propose a three-pronged education initiative, which includes:

- Grants by the National Science Foundation aimed at educating a new generation of professionals in information security and infrastructure protection.
- A series of conferences sponsored by the White House designed to spur new curricula in computer ethics and intellectual property for elementary and secondary schools.
- Partnership between the Department of Education and industry to develop curricula and market demand for educated and ethical technicians and managers.

Banking and Finance Findings and Recommendations

Beyond those already mentioned, we have a number of recommendations ranging through the areas of law enforcement, education and awareness, assistance to state and local governments, and many unique to certain infrastructures. But in the interest of time, I will focus briefly on those of specific interest to banking and finance.

At the outset, I want to acknowledge that we found that due to both effective regulation and industry diligence, individual institutions within the U.S. banking and financial system are more advanced than those in other sectors in their use of sophisticated tools and procedures to safeguard their operations from theft, fraud, and cyber crime. We applaud your vigilance in these areas.

We all know that both the financial service industry and government require strong public confidence—the industry in order to grow, and the government to sustain political viability. Each is central to the daily lives of virtually every American, and the degree of trust the public is willing to place in them depends directly on the reliability of the services provided. Infrastructure—as the carrier of the communications and transactions which deliver those services—is, therefore, critical to the performance of both.

But, as you well know, major trends of change—globalization, industry restructuring, Internet banking, and cyber cash—combine to create new risks. This is true within the financial services industry as well as the telecommunications and electric power industries upon which financial services heavily depend. These trends will result in new complexities and interdependencies, and hence new kinds of system-wide risks. These must be assessed carefully as you move forward.

The range of cyber threats for exploiting these vulnerabilities begins with the most likely but least consequential activities of hackers, and extends to the currently least likely but highest potential impact attack by a nation state or terrorist group. Current defenses against common hackers and criminals are quite good. However, it is the vulnerability to a possible coordinated attack on physical operations centers, or on the complex "system of systems" which enables this industry to function world-wide, that is of rising concern.

Some examples of specific actions to reduce these existing vulnerabilities include:

- Enhanced contingency planning throughout the financial system, including the use of strategic simulations to regularly test out such plans under a variety of circumstances.
- Geographic dispersion of such key industry utilities as clearing houses and depositories to mitigate the risk of physical attack.
- Availability of a government owned satellite-based communication system linking major money center banks with funds transfer and clearance centers for use in the event of catastrophic power or telecommunications outages.
- Continued improvement of internal controls and physical security measures.

- Establishment of a contingency data center for key industry messaging and data storage systems.

These recommendations represent the best case solutions for maximum security at the national level.

We acknowledge these might not pass muster as cost-beneficial investments at the individual institution level in the industry's risk management processes. At a minimum, therefore, we assume joint financing by government and industry. Some may even require full government funding if it is determined that the national security risks well exceed the reasonable business risk involved.

Standards

The Commission will recommend that government encourage and participate in the development of privately-established standards in those sectors where they are presently absent and, in those sectors where standards already exist, review them against national policy goals. The goal is voluntary standard-setting and adherence, not another big government mandate. The New York Federal Reserve's paper on "Sound Practices Guidance on Information Security" is exactly the type of effort that the Commission commends. This paper comprehensively defines the risks and problems you face and offers excellent advice on how to deal with them in ways that are both appropriate and effective.

Privacy Issues in the Employer-Employee Relationship

Throughout its year-long effort, the Commission has struggled to address the competing interests of security and privacy and the trade-offs between them. We have specifically studied the nexus of security and privacy in the employer-employee relationship. We will recommend that some of the tools that the federal government uses to perform background checks and issue security clearances be made available to employers within the critical infrastructures, at least in filling certain sensitive positions within those infrastructures. These would afford you the ability to inquire into and make use of criminal history information, employment histories, and credit history information. Amendments should also be made to federal polygraph law to include within the scope of current exemptions those who are in the business of providing information security services. These amendments would not make it mandatory that covered employers polygraph employees, but merely allow them to do so to the extent permitted under applicable state law.

Conclusion

Well, that was a quick trip through some of our activities. As you can see, we have been studying a wide range of issues and will have some fairly far-reaching and comprehensive conclusions. I hope this will add to your earlier discussions about the many dimensions of information security.

As a final note, this is the first time since I have been involved in government that I've seen the government actually trying seriously to get ahead of a problem before it becomes a crisis. We at the Commission know we are merely laying the foundation for long term efforts that will build upon our research and recommendations. But we know that we must take prudent steps now to protect and assure our nation's critical infrastructures.

This challenge requires a new way of thinking and creation of a new culture for both government and industry. Narrow point solutions are not the solution. Again, thank you for inviting me to join you today.
